Mutual authentication / cipher key delivery system

Publication number:	GB2279540 (A)
Publication date:	1995-01-04
Inventor(s):	TSUBAKIYAMA HIDEKI
Applicant(s):	KOKUSAI DENSHIN DENWA CO LTD [JP]
Classification:	
- international:	*G09C1/00; H04L9/06; H04L9/08; H04L9/14; H04L9/32; H04L12/22;* G09C1/00; H04L9/06; H04L9/08; H04L9/14; H04L9/32; H04L12/22; (IPC1-7): H04L9/32
- European:	H04L9/32B
Application number:	GB19940011680 19940610
Priority number(s):	JP19930163898 19930610

Also published as:

- GB2279540 (B)
- US5544245 (A)
- JP6350598 (A)

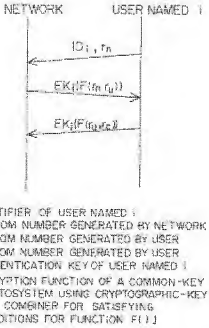
View INPADOC patent family

View list of citing documents

Abstract of **GB 2279540 (A)**

A network and each user i share an encryption algorithm EKi() using his authentication key Ki as a cipher key, its inverse function EKi-1(), a specific function F() and its inverse function F<1)<), and a function G(). The network calculates C1 = EKi(F(rn, ru)), using a random number rn generated by the user and a random number ru generated by the network, and sends it to the user. The user calculates (d1, d2) - F-1(EKi<-1)<C1)) and, if d1 = rn, judges the network to be an authorized one. The user generates a random number rc and sends C2 = EKi(F(d2, rc)) to the network. The network calculates (d3, d4) = F-1(EKi-1(C2)) and, if d3 = ru, judges the user to be an authorized one.

Fig. 1


NETWORK
USER NAMED i
IDi , rn
EKi(F(rn ru))
EKi(F(ru,rc))
IDi : IDENTIFIER OF USER NAMED i
ru : RANDOM NUMBER GENERATED BY NETWORK
rn : RANDOM NUMBER GENERATED BY USER
rc : RANDOM NUMBER GENERATED BY USER
Ki : AUTHENTICATION KEY OF USER NAMED i
EKi() : ENCRYPTION FUNCTION OF A COMMON-KEY CRYPTOSYSTEM USING CRYPTOGRAPHIC-KEY K,
F() : DATA COMBINER FOR SATISFYING (CONDITIONS FOR FUNCTION F( ))